

PATENT APPLICATION

**TECHNIQUE FOR MONITORING HEALTH OF NETWORK
DEVICE USING DATA FORMAT VERIFICATION**

Inventors: Gary Strawn
14920 Dark Star Court
Morgan Hill, CA 95037
Citizen of USA

Assignee: Cisco Technology, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

BEYER WEAVER & THOMAS, LLP
P.O. Box 778
Berkeley, CA 94704-0778
Telephone (510) 843-6200

TECHNIQUE FOR MONITORING HEALTH OF NETWORK DEVICE USING DATA FORMAT VERIFICATION

Inventors:

Gary Strawn
14920 Dark Star Court
Morgan Hill, CA 95037
Citizen of USA

Assignee:

Cisco Technology, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200

BACKGROUND OF THE INVENTION

Field of the invention

The present invention relates generally to data networks and more specifically to a technique for monitoring the health of network device using data format verification.

5 Background

Many of today's Internet content providers such as, for example, Yahoo.com, utilize a load-balanced server system in order to quickly provide desired content to a plurality of different users at substantially the same time. A block diagram of a conventional load-balanced server system is illustrated in FIGURE 1 of the drawings. As shown in FIGURE 1, a load-balanced server system 110 may be used by a content provider to respond to data requests from client devices (such as client device 102) via the Internet 104. The load-balanced server system 110 includes a load balancing device 106 and a plurality of server devices 108. The load balancing device 106 may be configured to perform the functions of a virtual server. When the virtual server receives a data request from the client device 102, it forwards the request to an appropriate server in the server farm 108.

According to conventional techniques, each of the servers in the server farm is periodically probed in order to determine whether the server is healthy and is operating properly. Conventionally, there are a variety of tests which may be performed in order to determine the health or status of a particular server in the server farm. As shown in the example FIGURE 1, health monitoring may be performed by a health monitoring agent or device 106a to determine which servers are active and healthy. For example, a selected server may be pinged in order to verify that the selected server is on-line.

A more qualitative status check involves transmitting a HTTP request to a selected server, and analyzing the data of the server's response in order to determine the health of the selected server. For example, a health monitoring device may transmit an HTTP request to a selected server to thereby cause the server to transmit an HTTP response to the health monitoring device. The data from the HTTP response may then be analyzed to determine whether the selected server is healthy and functioning properly.

Typically, the health monitor knows what to request and only vaguely what kind of response to expect. For example, when verifying an HTTP reply, the HTTP reply codes

can be checked for error values in the header portion of the HTTP response to determine the relative health or status of the server. However, the error codes can not be used to verify that the retrieved resource is completely valid.

According to an alternate technique, the HTTP request submitted by the health monitoring device includes a request for the selected server to transmit an HTTP response which includes static HTML data such as, for example, a static HTML page. When the health monitoring device receives the static HTML data, it may then perform content verification of the static HTML data to determine whether the selected server is functioning properly. Typically, content verification is performed by comparing the received static HTML data to preconfigured HTML data stored at the health monitoring device. Thus, for example, the health monitoring device may check the health of a selected server by submitting a request to the server to transmit a specific, static HTML page used for test purposes. If the server is healthy, it should be able to transmit the requested test HTML page to the health monitoring device. The health monitoring device expects to receive specific HTML data from the selected server in response to the health status request. Thus, when the health monitoring device receives the test HTML data from the selected server, it compares the received HTML data to preconfigured HTML data stored at the health monitoring device to thereby verify the accuracy of the content of the test HTML page.

One problem with the above-described server health monitoring technique is that it does not allow verification of non-deterministic responses, such as CGI generated responses. Additionally, conventional server health monitoring techniques are ineffective when used to verify the contents of customized or dynamically generated data. One reason why a conventional health monitoring device is unable to perform this function is that the specific content of a customized or dynamically generated HTML page typically cannot be predetermined. Since the health monitoring device does not know the specific content which it expects to receive, it is unable to perform content verification, and is therefore unable to determine whether the server is functioning properly.

In order to partially overcome the above-described problems, conventional server health monitoring techniques have attempted to perform content verification of customized or dynamically generated HTML pages by checking for static content which is expected to be included in each requested HTML page. For example, a content provider such as

Yahoo.com may include the text "copyright Yahoo.com" on each customized or dynamically generated web page. Thus, when the health monitoring device requests, for example, a dynamically generated web page from a selected Yahoo server, it may determine the health of the server by verifying the static portion (e.g. "copyright
5 Yahoo.com") of the content of the dynamically generated HTML page. However, this modified technique of server health verification remains ineffective for verifying non-deterministic data such as customized or dynamically generated data.

While conventional techniques for monitoring the health of selected servers in a load-balanced server system have improved, there currently exists a number of problems
10 which still need to be addresses. Accordingly, there exists a continual need to improve upon network device health monitoring techniques.

SUMMARY OF THE INVENTION

According to specific embodiments of the present invention, a method and
15 computer program product are disclosed for determining a health status of a selected network device in a data network. A resource request is transmitted to the selected network device. Data including content information is then received from the network device in response to the resource request. At least a portion of the content information is verified by verifying at least one format of a selected portion of content information using
20 format verification rules. According to a specific implementation, the format verification rules may include pre-defined regular expressions. Additionally, according to a specific implementation, verification of the content information may include determining whether any inconsistencies are detected in any of the formats of the selected content information being analyzed. The health status of the network device may then be determined based
25 upon the results of the content verification.

Alternate embodiments of the present invention are directed to a method and computer program product for performing content verification of data received from a selected network device. The data received from the selected network device includes content information. At least a portion of the content information is verified by verifying
30 at least one format of a selected portion of the content information using pre-defined format verification rules. In performing the content verification, a determination may be

made as to whether any inconsistencies are detected in at least one format of the selected content information being analyzed.

Other embodiments of the present invention are directed to a method and computer program product for determining a health status of a selected network device in a data network. A resource request is transmitted to the selected network device. Data, including content information, is received from the network device in response to the resource request. At least one format of a selected portion of the content information is verified using format verification rules. According to a specific embodiment, the format verification includes determining whether there are any inconsistencies in any of the formats of the selected content information. Thereafter, the health status of the selected network device may be determined based upon the results of the format verification of the received data.

An alternate embodiment is directed to a system for determining a health status of a selected network device in a data network. The system comprises at least one CPU, memory which is adapted to store format verification rules, and at least one interface for communicating with the selected network device. The system may be configured to transmit a resource request to the selected network device. The system may also be configured to receive data from the network device in response to the resource request. The received data may include content information. The system is also configured to verify at least a portion of the content information by verifying at least one format of a selected portion of the content information using the format verification rules. According to a specific implementation, the format verification rules may include pre-defined regular expressions. The system may further be configured to determine the health status of the network device based upon the results of the content verification analysis.

Another embodiment of the present invention is directed to a system for performing content verification of data received from a selected network device. The system comprises at least one CPU, memory adapted to store format verification rules, and at least one interface for communicating with the selected network device. The system is configured to receive data from the network device. The data may include content information such as, for example, HTML data. The system may be further configured to verify at least a portion of the content information by verifying at least one format of a selected portion of the content information using the format verification rules. The system

may also be configured to determine whether any inconsistencies are detected in the formats of the selected content information being verified.

A different embodiment of the present invention is directed to a system for determining a health status of a selected network device in a data network. The system comprises at least one CPU, memory adapted to store format verification rules, and at least one interface for communicating with the selected network device. The system may be configured to transmit a resource request to the selected network device, and may be configured to receive data from the network device in response to the resource request. The data may include content information. The system may further be configured to verify at least one format of a selected portion of the content information using pre-determined format verification rules. The format verification may include determining whether any inconsistencies are detected in any of the formats of the selected content information being analyzed. The system may also be configured to determine whether the network device is functioning properly based upon the results of the format verification analysis.

Additional objects, features and advantages of the various aspects of the present invention will become apparent from the following description of its preferred embodiments, which description should be taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGURE 1 shows a block diagram of a data network which may be used for implementing the technique of the present invention.

FIGURE 2 shows a flow diagram of a Server Health Monitoring Procedure 200 in accordance with a specific embodiment of the present invention.

FIGURE 3 shows a flow diagram of a Content Verification Procedure 300 in accordance with a specific embodiment of the present invention.

FIGURE 4 shows a network device 60 suitable for implementing the network device health monitoring technique of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

FIGURE 2 shows a flow diagram of a Server Health Monitoring Procedure 200 in accordance with a specific embodiment of the present invention. According to a specific implementation, the Server Health Monitoring Procedure may be implemented by a health

monitoring device or agent such as agent 106a of FIGURE 1. It will be appreciated that the health monitoring technique of the present invention may be used to monitor the health of any network device which transmits data that conforms with a standardized or recognizable format. For purposes of illustration, it is assumed that the Server Health Monitoring Procedure 200 of FIGURE 2 is used to monitor the health of a particular server (e.g. 106a) of the load-balanced server farm 110 of FIGURE 1.

As shown at 202 of FIGURE 2, a specific network device (e.g. Server A 108a, FIGURE 1) is selected for health monitoring analysis. An attempt is then made (204) to connect to the selected server. If no connection to the server has been made within a first pre-determined time period (which may be a configurable parameter), then it may be determined (206) that the connection attempt to the server has timed out. Accordingly, the connection time out error is reported (218) to an appropriate location for handling.

Assuming that the health monitoring device establishes a connection to the selected server, the health monitoring device may then send (208) a "Get Resource" request to the selected server in order to retrieve desired data from the selected server relating to a desired file or resource to be analyzed to content or format verification. For example, the "Get Resource" request may include an HTTP request to receive data associated with a specific URL such as, for example, a URL corresponding to a specific web or HTML page. If the health monitoring device does not receive a response from the selected server within a second pre-determined time period (which may be a configurable parameter), the health monitoring device may determine (210) that the "Get Resource" request has timed out. Accordingly, the Get Resource time out error is reported (218) to an appropriate location for handling.

At 212 it is assumed that a response from the selected server has been received at the health monitoring device. For example, the response may be an HTTP response which includes data such as, for example, HTML data, JPEG data, or other content information corresponding to the URL specified in the Get Resource request.

According to a specific embodiment, once the response to a Get Resource request has been received by the health monitoring device, content verification of the received data may be performed (214) by verifying the format(s) of all or a selected portion of the received data using pre-defined format verification rules. According to a specific implementation, verification of the received data using the pre-defined format verification

rules may be accomplished by implementing the Content Verification Procedure 300 of FIGURE 3 (described in greater detail below).

According to a specific embodiment, the pre-defined format verification rules may include regular expressions. As commonly known to one having ordinary skill in the art, regular expressions are patterns of text which may include ordinary characters (e.g. A-Z) and special characters known as metacharacters. A regular expression specifies a pattern which describes one or more strings to match when searching a body of text. Thus, for example, a regular expression may serve as a template for matching a character pattern to one or more strings which are located in the body of the text. A more detailed description of format verification using regular expressions is provided with respect to FIGURE 3 of the drawings.

Using the results of the data content verification, a determination may then be made (216) as to whether the selected server is healthy or functioning properly. Assuming that there are no errors detected in the format of the received data, the health monitoring device may conclude that the selected server is healthy (e.g., functioning properly). Thereafter, the health monitoring device may select a different server or other network device for health monitoring analysis.

If, however, at least one error is detected in the format of the received data, the health monitoring device may conclude that the selected server is not healthy or is not functioning properly, and may then report (218) the error to an appropriate location for handling. According to a specific implementation, any errors detected by the health monitoring device may be reported to a user, system administrator, and/or another network device for handling. In one implementation, if an error has been reported for a selected server, that server may be taken off line.

According to a specific implementation, separate threads of the Server Health Monitoring Procedure may be implemented concurrently in order to monitor the health status of several network devices at the same time.

FIGURE 3 shows a flow diagram of a Content Verification Procedure 300 in accordance with a specific embodiment of the present invention. According to one embodiment, the Content Verification Procedure 300 may be implemented by the health monitoring device during its verification of content of data received from a selected network device. As shown at 302 at FIGURE 3, content verification is achieved using

format verification, which may be performed on all or a selected portion of the received data by applying predefined format verification rules to the received data. According to a specific implementation, the format verification rules may be achieved using regular expressions. Examples of regular expressions are provided below.

- 5 When the health monitoring device receives a response form the selected server, it can use pre-defined regular expressions to determine whether or not the received response is valid by validating the format of the response data, rather than by validating the content of the actual data itself.

- 10 It will be appreciated that regular expressions are very flexible and powerful in their ability to verify a resource. Using regular expressions, a user is able to configure a health monitoring device to verify the format of non-deterministic data such as, for example, the customized or dynamically generated content data of any web page. In this way, content verification of a web page or other resource file may be performed without knowing what the actual content of the resource file should be.

- 15 According to a specific embodiment, regular expressions may be configured using an operating system command set language such as, for example, Cisco System's IOS command set. This provides for a simple user interface and allows configuration through a telnet or similar command-line connection.

- 20 Returning to FIGURE 3, at 306 a determination is made as to whether any inconsistencies have been detected in the format verification analysis of the received data. If no inconsistencies have been detected, then the Content Verification Procedure 300 may return a "status OK" message (308). If, however, at least one inconsistency is detected in the format of the received data, the Content Verification Procedure may report a "status error" message (310). According to a specific implementation, any status message
25 reported by the Content Verification Procedure may be reported to the Server Health Monitoring Procedure in order to allow the Server Health Monitoring Procedure to determine whether the selected server or network device is healthy and/or functioning properly.

Illustrative Examples

The following examples are intended to help provide the reader with a better understanding of the network device health monitoring technique of the present invention using format verification rules.

5 Example 1

In a first example, it is assumed that it is desired to perform a health monitor status check on a web server which returns a web page with the current time on it (herein referred to as a "current time" web page). In this first example, it is further assumed that the current time web page reports the time in the following format: HH:MM AM/PM, where
10 HH denotes the hours portion of the current time, and MM denotes the minutes portion of the current time.

In this example, the web page is an HTML page which is dynamically generated by the server each time it receives a specific request for that page. Using conventional health monitoring techniques, it would not be possible for the health monitoring device to verify
15 that a valid time was returned since the content of the web page is continuously changing. However, using the technique of the present invention, the health of the web server may be determined by verifying the format of the data of the current time web page. For example, the format of the time information of the requested web page may be verified using a regular expression, as shown below:

20
$$([1-9]|1[0-2]):[0-5][0-9] (A|P)M \quad (1)$$

Using the above regular expression as shown at (1), the time data of the current time web page must meet the following criteria in order to be validated. The hours portion of the time value (e.g., HH) must be an integer from 1 to 12, inclusive. This number must be followed by a colon. The minutes portion of the time value (e.g., MM) must then be a
25 number from 0 to 59, inclusive. The time data string must then be followed by the characters "AM" or "PM".

Thus, for example, according to the regular expression defined in (1), the health monitoring device will validate a string such as "3:06 PM," but would not validate a data string such as "0:83 KM." If the health monitoring device determines that the format of
30 the time data string is invalid, it will assume that the web server is not functioning properly, and will report an error to an appropriate device or location.

Example 2

In this second example, it is assumed that a web server is configured to return a web page which contains at least one stock symbol and its respective current dollar value. Using conventional health monitoring techniques, a simple text verification search can not be used to verify the content of this web page since there is no way to know what ticker symbol the user will request or what the corresponding dollar value will be. However, using the technique of the present invention, it is possible to validate the information returned by the server by validating the format of the returned data.

Thus, using the technique of the present invention, a health monitoring device is able to validate the information returned by the server by validating the format of at least a portion of the information. If there are no inconsistencies the format of the analyzed data, then the health monitoring device may conclude that the web server is healthy and functioning properly. An example of a regular expression which may be used to validate a stock symbol and dollar amount is shown below:

$$([A-Z]{1,4}|[A-Z]{4}X) (\$0[1-9][0-9]^*.[0-9]{2}) \quad (2)$$

In the example above, it is assumed that the web server will return a web page which includes a ticker symbol followed by the dollar price. According to the regular expression rules defined in (2), the ticker symbol must have a length of 1-4 characters, or must have a length of five characters with the last character being an "X." Further, the dollar value must include the dollar sign followed by a number which can be 0 or positive (but can not have leading zeros), followed by a decimal point, followed by two more numeric digits. Thus, for example, using the regular expression rules defined in (2), the health monitor would validate a string such as "CSCO \$100.00", but would not validate a data string such as "CCSCO \$1F".

It will be appreciated that one or more desired format verification rules may be applied to any given data string in order to verify the content of such data. For example, a Get Resource request from the health monitoring device may specify a specific web page which includes both a current time stamp and at least one stock ticker symbol. In this situation, both of the regular expressions (1) and (2) may be used to verify the format of the data corresponding to the requested web page.

A more detailed discussion of regular expressions and their use is provided in the book entitled "Compilers, Principles, Techniques, and Tools," by Alfred V. Aho, Bell

Telephone Laboratories, Inc., 1988, which is incorporated herein by reference in its entirety for all purposes.

Other Embodiments

Generally, the network device health monitoring technique of the present invention may be implemented on software and/or hardware. For example, it can be implemented in an operating system kernel, in a separate user process, in a library package bound into network applications, on a specially constructed machine, or on a network interface card. In a specific embodiment of this invention, the technique of the present invention is implemented in software such as an operating system or in an application running on an operating system.

A software or software/hardware hybrid implementation of the network device health monitoring technique of this invention may be implemented on a general-purpose programmable machine selectively activated or reconfigured by a computer program stored in memory. Such programmable machine may be a network device designed to handle network traffic, such as, for example, a router or a switch. Such network devices may have multiple network interfaces including frame relay and ISDN interfaces, for example. Specific examples of such network devices include routers and switches. For example, the network devices implementing this invention may be specially configured routers or servers such as specially configured router models 1600, 2500, 2600, 3600, 4500, 4700, 7200, 7500, and 12000 available from Cisco Systems, Inc. of San Jose, California, or may be specially configured switches such as the specially configured switch model Catalyst 6000, available from Cisco Systems, Inc. A general architecture for some of these machines will appear from the description given below. In an alternative embodiment, the network device health monitoring technique of this invention may be implemented on a general-purpose network host machine such as a personal computer or workstation. Further, the invention may be at least partially implemented on a card (e.g., an interface card) for a network device or a general-purpose computing device.

Referring now to FIGURE 4, a network device 60 suitable for implementing the network device health monitoring technique of the present invention includes a master central processing unit (CPU) 62, interfaces 68, and a bus 67 (e.g., a PCI bus). When acting under the control of appropriate software or firmware, the CPU 62 may be

responsible for implementing specific functions associated with the functions of a desired network device. For example, when configured as a load balancing device, the CPU 62 may be responsible for analyzing packets, encapsulating packets, forwarding packets to appropriate network devices, performing content and/or format verification of data, etc.

- 5 The CPU 62 preferably accomplishes all these functions under the control of software including an operating system (e.g. Windows NT), and any appropriate applications software.

CPU 62 may include one or more processors 63 such as a processor from the Motorola family of microprocessors or the MIPS family of microprocessors. In an
10 alternative embodiment, processor 63 is specially designed hardware for controlling the operations of network device 60. In a specific embodiment, a memory 61 (such as non-volatile RAM and/or ROM) also forms part of CPU 62. However, there are many different ways in which memory could be coupled to the system. Memory block 61 may be used for a variety of purposes such as, for example, caching and/or storing data,
15 programming instructions, etc.

The interfaces 68 are typically provided as interface cards (sometimes referred to as "line cards"). Generally, they control the sending and receiving of data packets over the network and sometimes support other peripherals used with the network device 60. Among the interfaces that may be provided are Ethernet interfaces, frame relay interfaces,
20 cable interfaces, DSL interfaces, token ring interfaces, and the like. In addition, various very high-speed interfaces may be provided such as fast Ethernet interfaces, Gigabit Ethernet interfaces, ATM interfaces, HSSI interfaces, POS interfaces, FDDI interfaces and the like. Generally, these interfaces may include ports appropriate for communication with the appropriate media. In some cases, they may also include an independent processor
25 and, in some instances, volatile RAM. The independent processors may control such communications intensive tasks as packet switching, media control and management. By providing separate processors for the communications intensive tasks, these interfaces allow the master microprocessor 62 to efficiently perform routing computations, network diagnostics, security functions, etc.

30 Although the system shown in FIGURE 4 illustrates one specific network device of the present invention, it is by no means the only network device architecture on which the present invention can be implemented. For example, an architecture having a single

processor that handles communications as well as routing computations, etc. is often used. Further, other types of interfaces and media could also be used with the network device.

Regardless of network device's configuration, it may employ one or more memories or memory modules (such as, for example, memory block 65) configured to store data, program instructions for the general-purpose network operations and/or other information relating to the functionality of the network device health monitoring technique described herein. The program instructions may control the operation of an operating system and/or one or more applications, for example. The memory or memories may also be configured to include data structures which store regular expressions and other format verification rules, content data received from selected network devices, etc.

Because such information and program instructions may be employed to implement the systems/methods described herein, the present invention relates to machine readable media that include program instructions, state information, etc. for performing various operations described herein. Examples of machine-readable media include, but are not limited to, magnetic media such as hard disks, floppy disks, and magnetic tape; optical media such as CD-ROM disks; magneto-optical media such as floptical disks; and hardware devices that are specially configured to store and perform program instructions, such as read-only memory devices (ROM) and random access memory (RAM). The invention may also be embodied in a carrier wave travelling over an appropriate medium such as airwaves, optical lines, electric lines, etc. Examples of program instructions include both machine code, such as produced by a compiler, and files containing higher level code that may be executed by the computer using an interpreter.

Although several preferred embodiments of this invention have been described in detail herein with reference to the accompanying drawings, it is to be understood that the invention is not limited to these precise embodiments, and that various changes and modifications may be effected therein by one skilled in the art without departing from the scope of spirit of the invention as defined in the appended claims.